



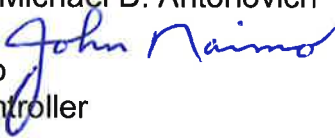
JOHN NAIMO
AUDITOR-CONTROLLER

**COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER**

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

October 13, 2016

TO: Supervisor Hilda L. Solis, Chair
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Don Knabe
Supervisor Michael D. Antonovich

FROM: John Naimo 
Auditor-Controller

SUBJECT: **CHILD SUPPORT SERVICES DEPARTMENT – INFORMATION
TECHNOLOGY AND SECURITY REVIEW**

The Board of Supervisors' (Board) Information Technology (IT) and Security Policies (Policies) require all County departments to comply with established Countywide IT security standards to help ensure proper controls over County IT resources. As required by Board Policy 6.108, we are reviewing County departments' compliance with the Policies.

We have completed a review of the Child Support Services Department's (CSSD or Department) compliance with the Policies, and related County standards and County Fiscal Manual (CFM) requirements. CSSD uses two mission-critical systems, including the Child Support Enforcement (CSE) System and the Medi-Cal Eligibility Data System (MEDS), to manage participants' personal and Medi-Cal case information, respectively. CSSD also reported having over 1,900 IT devices, such as desktop computers, laptops, and servers. Our review included testing IT access controls, encryption and antivirus protection, equipment control, equipment disposition, and security awareness training.

Results of Review

Our review disclosed that CSSD needs to improve its controls over areas such as IT access controls, equipment control, and encryption and antivirus protection. The following are examples of areas for improvement:

- **Inappropriate Access** – CSSD needs to restrict users' CSE, MEDS, and Virtual Private Network (VPN) access. We noted that the access for 60 users (29 CSE and 31 MEDS) remained active for up to seven years after they terminated from CSSD. In addition, 24 other users (20 CSE and four VPN) had active access that they never used. The access to these systems allows users to view, enter, and update participants' personal and Medi-Cal case information, increasing the risk of exposure.

CSSD's attached response indicates that they have deactivated or restricted the access rights for all 60 users who terminated and have implemented changes to their internal staffing system to ensure CSE and MEDS access is removed timely when employees leave the Department. CSSD also indicated that they reviewed the system access needs of the 24 individuals who never used their access and took appropriate action.

- **Encryption and Antivirus Protection** – CSSD needs to ensure all computing devices are encrypted and have current antivirus protection. Of the 40 devices reviewed, we noted 11 (28%) were missing encryption and/or current antivirus protection, including five laptops that were missing both. We also noted that three (8%) laptops were damaged and would not turn on, or had an obsolete operating system that prevented staff from installing and/or updating the security software. These devices should have been dispositioned and removed from inventory as required by CFM Section 5.3.2.

CSSD's attached response indicates that they have ensured all desktops, and the laptops that are currently in use, are encrypted. They also told us that they have reviewed all desktops and 70% of their laptops to ensure they have current antivirus protection. CSSD is working to ensure the remaining devices are also appropriately protected. CSSD's response also indicates that they have established procedures to regularly monitor encryption and antivirus protection on their devices, and that they will review the damaged laptops noted in our review and repair or salvage them as necessary.

- **IT Equipment Inventory** – CSSD needs to inventory their IT equipment annually and update inventory records with the results of the physical counts. We noted one (5%) of the 20 IT devices we randomly sampled was missing from their IT equipment list. CSSD management also indicated that they did not complete a physical inventory of IT devices in calendar year 2015 as required.

CSSD's attached response indicates that they performed a new physical inventory count and are in the process of reconciling the count to their former equipment inventory. CSSD will also ensure they conduct annual physical inventories and maintain updated inventory records.

- **Secured Disposition of IT Devices** – CSSD needs to maintain documentation to support that their computing devices and any data/software stored on them are rendered unreadable and unrecoverable (i.e., sanitized) before disposing of the devices from County inventory. We noted eight (80%) of the ten computing devices reviewed were missing documentation to support that the devices were sanitized before they were donated. One of the laptops was also missing documentation to support that the device was actually donated or properly disposed.

CSSD's attached response indicates that staff in their Chief Technology Office have confirmed their acknowledgement and understanding of the department's sanitization policy and related documentation requirements. CSSD has also established procedures to maintain complete records supporting the sanitization and donation of computing devices.

Details of these and other findings and recommendations are included in Attachment I.

Review of Report

We discussed the results of our review with CSSD management. CSSD's attached response (Attachment II) indicates general agreement with our findings and recommendations.

We thank CSSD management and staff for their cooperation and assistance during our review. If you have any questions please call me, or your staff may contact Robert Smythe at (213) 253-0100.

JN:AB:PH:RS:MP

Attachments

c: Sachi A. Hamai, Chief Executive Officer
Dr. Steven J. Golightly, Director, Child Support Services Department
Dr. Robert K. Pittman, Chief Information Security Officer, Chief Executive Office
Public Information Office
Audit Committee

CHILD SUPPORT SERVICES DEPARTMENT INFORMATION TECHNOLOGY AND SECURITY REVIEW

Background

The Board of Supervisors' (Board) Information Technology (IT) and Security Policies (Policies) require departments to comply with minimum IT security standards. The Policies help protect County IT assets and ensure the confidentiality and integrity of systems data. As required by Board Policy 6.108, we are reviewing County departments' compliance with the Policies.

We have completed a review of the Child Support Services Department's (CSSD or Department) compliance with the Policies, and related County standards and County Fiscal Manual (CFM) requirements. CSSD uses two mission-critical systems, including the Child Support Enforcement (CSE) System and the Medi-Cal Eligibility Data System (MEDS), to manage participants' personal and Medi-Cal case information, respectively. CSSD also reported having over 1,900 IT devices, such as desktop computers, laptops, and servers. Our review included testing IT access controls, encryption and antivirus protection, equipment control, equipment disposition, and security awareness training.

Access Controls

Board Policy 6.101 requires departments to establish access controls to protect against unauthorized access, use, exposure, disclosure, modification, or destruction of County IT resources. CFM Section 8.7.4.2 also requires departments to limit unneeded access by immediately updating user access rights when employees terminate or change job duties, and by periodically reviewing the propriety of users' access levels.

Inappropriate Access

We reviewed CSSD users' Virtual Private Network (VPN) access and system access for two of the Department's mission-critical systems, including CSE and MEDS. We noted numerous instances of inappropriate user accounts. Specifically:

- **Terminated Employees with Access** – Access for 60 users (29 CSE and 31 MEDS) remained active for up to seven years after they terminated from CSSD. The access to these systems allows users to view, enter, and update participants' personal and Medi-Cal case information. CSSD needs to immediately remove terminated and transferred employees' user access, and remind staff to remove future terminated and transferred employees' user access timely.
- **Unused Access** – 24 other users, including 20 CSE users and four VPN users, have never used their access, and four additional VPN users have not used their access in over a year and may not need it. CSSD should review the 28 users noted in our review and remove all unnecessary access.

CSSD also does not have written procedures to periodically review all users' VPN, CSE, and MEDS access as required by CFM Section 8.7.4.2. To ensure access is consistent with users' job duties, CSSD needs to establish written procedures to periodically review users' VPN, CSE, and MEDS access.

Recommendations

Child Support Services Department management:

- 1. Immediately remove terminated and transferred employees' user access, and remind staff to remove future terminated and transferred employee's user access timely.**
- 2. Review the 28 users noted in our review and remove all unnecessary access.**
- 3. Establish written procedures to periodically review all users' Virtual Private Network, Child Support Enforcement System, and Medi-Cal Eligibility Data System access.**

Password Protection

CSSD procedures require all systems that process and/or store child support information to force users to change their passwords every 60 days. We noted that CSSD stores participant case information on their Department network, which requires password changes every 90 days, exceeding the Department's 60-day requirement. To protect child support information in compliance with the Department's procedures, CSSD should ensure network settings require users to change their passwords every 60 days.

Also, during our review of CSSD's IT equipment (as discussed in the IT Equipment Inventory section below), we noted an instance where staff taped their user identification and password on their computer, in violation of CFM Section 8.7.4.3. To help prevent unauthorized access and protect County data, CSSD should remind employees to keep their user identification and password secured.

Recommendations

Child Support Services Department management:

- 4. Ensure network settings require users to change their passwords every 60 days.**
- 5. Remind employees to keep their user identification and password secured.**

Encryption and Antivirus Protection

Board Policy 6.110 requires departments to encrypt all County portable computers. Encryption protects against unauthorized disclosure of personal/confidential information if a computer is lost or stolen. Board Policy 6.102 requires departments to ensure computing devices have antivirus protection that is updated when a new software version and/or detection definition file is available.

CSSD staff generally install encryption and antivirus protection on computing devices during the software setup process before the devices are given to Department personnel. However, of the 40 assigned devices selected for testing, we noted that:

- Eleven (28%) devices were missing encryption and/or current antivirus protection, including five laptops that were missing both. We noted antivirus definitions were at least one month old with the oldest being from October 2013. Three of the laptops also had antivirus software that was no longer supported, which prevents devices from obtaining the latest virus definitions.

To prevent the unauthorized use or disclosure of County information, CSSD needs to ensure all computing devices have encryption and current antivirus protection as required by the Policies.

- Three (8%) laptops were damaged and would not turn on, or had an obsolete operating system that prevented staff from installing and/or updating the security software. These devices should have been dispositioned and removed from inventory as required by CFM Section 5.3.2. CSSD needs to ensure damaged and obsolete equipment is properly disposed and removed from inventory.

CSSD also does not have a process in place to regularly monitor encryption and antivirus protection on their devices. However, we noted the encryption and antivirus software can produce reports that could be used, along with CSSD's IT equipment list, to monitor device protection. CSSD should evaluate using encryption and antivirus reports, along with the IT equipment list, to monitor encryption and antivirus protection on all their computing devices.

Recommendations

Child Support Services Department management:

6. **Ensure all computing devices have encryption and current antivirus protection as required by the Policies.**
7. **Ensure damaged and obsolete equipment is properly disposed of and removed from inventory.**

8. **Evaluate using encryption and antivirus reports, along with the IT equipment list, to monitor encryption and antivirus protection on all their computing devices.**

IT Equipment Inventory

CFM Section 6.8.2 requires departments to conduct a physical inventory of all non-capital assets at least once each year, and reconcile the inventory to the department's listing of non-capital asset equipment.

We noted one (5%) of the 20 IT devices we randomly sampled was missing from CSSD's IT equipment list. CSSD management also indicated that they did not complete a physical inventory of IT devices in calendar year 2015 as required. CSSD needs to inventory all IT equipment immediately, and annually thereafter, and update inventory records with the results of the physical counts.

Recommendation

9. **Child Support Services Department management inventory all information technology equipment immediately, and annually thereafter, and update inventory records with the results of the physical counts.**

Secured Disposition of IT Devices

Board Policy 6.112 requires departments to render all data and software from computer hard drives unreadable and unrecoverable (i.e., sanitize) before disposing of the device from County inventory. CSSD procedures also require that staff document the sanitization and donation of computing devices.

We selected ten computing devices from the Department's donated IT equipment list and noted that eight (80%) devices were missing documentation to support that they were sanitized before they were donated. This includes one laptop that was also missing documentation to support that the device was actually donated or properly disposed.

Without proper documentation, CSSD management cannot ensure that the devices, and any County software and/or child support information stored on them, are sanitized and disposed as required. CSSD needs to maintain documentation to support the sanitization and donation of computing devices.

Recommendation

10. **Child Support Services Department management maintain documentation to support the sanitization and donation of computing devices.**

IT Security Awareness Training

Board Policy 6.111 requires departments to provide IT security awareness training to all staff at the time they are hired and annually thereafter. We reviewed CSSD's training records and noted that 83 (6%) of the 1,451 CSSD employees have not completed the required training in at least a year. The lack of training can contribute to some of the weaknesses noted in our review, such as the inappropriate access noted in the Access Controls section above. CSSD management needs to ensure all employees complete the required information security awareness training when hired and annually thereafter.

Recommendation

- 11. Child Support Services Department management ensure all employees complete the required Information Security Awareness Training when hired and annually thereafter.**

IT Risk Assessment

Board Policy 6.107 requires that departments perform risk assessments on their critical IT services by properly completing the Auditor-Controller's Internal Control Certification Program (ICCP). Departments must certify that proper controls are in place, or that action is being taken to correct any weaknesses or vulnerabilities.

We noted that CSSD completed the ICCP, but did not identify CSE and MEDS as critical IT systems. These systems are used to manage participants' personal and Medi-Cal case information, which are critical to the Department's mission. To help assess and improve controls over IT security, CSSD management needs to perform risk assessments on all their critical systems by properly completing the ICCP.

Recommendation

- 12. Child Support Services Department management perform risk assessments on all critical systems by properly completing the Internal Control Certification Program.**



County of Los Angeles
Child Support Services Department



STEVEN J. GOLIGHTLY, Ph.D.
Director

DEAN DE GRUCCIO
Chief Deputy Director

September 22, 2016

TO: John Naimo
Auditor-Controller

FROM: Steven J. Golightly, Ph.D.
Director

A handwritten signature in black ink, appearing to read "S. Golightly".

SUBJECT: **CHILD SUPPORT SERVICES DEPARTMENT'S RESPONSE TO
AUDITOR-CONTROLLER'S INFORMATION TECHNOLOGY AND
SECURITY REVIEW**

Attached is the Los Angeles County Child Support Services Department's response to the recommendations contained in the Auditor-Controller's Information and Technology and Security Review. We concur with the findings and all of the recommendations have been either fully or partially implemented.

We appreciate the opportunity to include our response in your report and thank your staff for their professionalism in conducting their review of our operation. Please let me know if you have any questions or require additional information. You may also contact Administrative Deputy Rosemary Gutierrez at (323) 889-2981 or Chief Financial Officer Barbara Rankin at (323) 889-3460.

SJG:RG:BR:rk

c: Rosemary Gutierrez
Alexandra Bauer
Hooman Hassanpour

Attachment

EXECUTIVE OFFICES

5770 S. Eastern Avenue • Commerce, CA 90040 • (323) 889-3400

*"To enrich our community by providing child support services
in an efficient, effective and professional manner, one family at a time"*

**LOS ANGELES COUNTY CHILD SUPPORT SERVICES DEPARTMENT
RESPONSE TO AUDITOR-CONTROLLER'S INFORMATION TECHNOLOGY AND
SECURITY REVIEW**

AUDITOR-CONTROLLER RECOMMENDATION #1

Immediately remove terminated and transferred employees' user access and remind staff to remove future terminated and transferred employee's user access timely.

Child Support Services Response:

The Child Support Services Department agrees and is in the process of implementing this recommendation. Regarding terminated and transferred employees who still had access to the CSE and MEDS systems, the following information has been confirmed:

- Out of the 29 CSE accounts that had not been deactivated, 21 of the accounts were deactivated as of July 6, 2016. The remaining 8 accounts still had active cases assigned to the users. All access rights granted to these accounts were removed and the accounts were listed on a tracking log to be monitored until the cases are reassigned.
- Changes were made to the CSSD Human Resources Item Control system to ensure that CSSD Help Desk personnel are properly notified when an employee leaves the department so that access to department systems can be removed promptly. In situations where CSE accounts cannot be closed immediately due to active cases being assigned to that account, all access will be immediately removed from those accounts and the accounts will be added to the tracking log. This log will be monitored by the Help Desk supervisor, who will deactivate the accounts once all active cases have been reassigned.
- For all of the MEDS accounts that had not been deactivated, a request to deactivate these accounts was sent to the State of California Department of Child Support Services on July 6, 2016.

AUDITOR-CONTROLLER RECOMMENDATION #2

Review the 28 users noted in the review and remove all unnecessary access.

Child Support Services Response:

The Child Support Services Department agrees and has fully implemented this recommendation. The review of the 28 users and the appropriate actions was completed by September 9, 2016.

AUDITOR-CONTROLLER RECOMMENDATION #3

Establish written procedures to periodically review users' Virtual Private Network, Child Support Enforcement System, and Medical Eligibility Determination System access.

Child Support Services Response:

The Child Support Services Department agrees and is in the process of implementing this recommendation. The Chief Technology Office Help Desk is establishing written documentation regarding the procedures to follow when reviewing a user's access rights to the Child Support Enforcement system, Medical Eligibility Determination System, and Virtual Private Network. This analysis will be performed twice; once after the procedures are set, and then again on an individual basis when a user's job function changes.

AUDITOR-CONTROLLER RECOMMENDATION #4

Ensure network settings require users to change their password every 60 days.

Child Support Services Response:

The Child Support Services Department agrees and has fully implemented this recommendation. The setting for "Maximum Password Age" in CSSD's Active Directory was changed to 60 days on August 29, 2016. This setting change requires users to change their passwords every 60 days.

AUDITOR-CONTROLLER RECOMMENDATION #5

Remind employees to keep their user identification and passwords secured.

Child Support Services Response:

The Child Support Services Department agrees and has fully implemented this recommendation. An email from the Child Support Services Department's Chief Technology Officer was sent on July 5, 2016 to all personnel and a reminder notice will be distributed every six months to all staff. The importance of not writing down user IDs and passwords was reiterated and the instructions on managing passwords through CSSD's Single Sign On system were reissued to all personnel in this email.

AUDITOR-CONTROLLER RECOMMENDATION #6

Ensure all computer devices have encryption and current antivirus protection as required by the Policies.

Child Support Services Response:

The Child Support Services Department agrees and is in the process of implementing this recommendation. Regarding the encryption of all computing devices and the update of antivirus protection the following actions have been taken:

- Encryption was verified on all desktop workstations on June 17, 2016.
- All laptops currently in use were verified encrypted June 23, 2016. All laptops in storage are currently undergoing verification. Expected completion is September 30, 2016.
- New procedures were implemented for the updating and encrypting of all laptops. All laptops, including those in storage and those checked out by users, will be checked every two months to verify that antivirus software has been updated and that the hard drives are encrypted.
- The progress of all laptops is currently at 70% completion. The expected completion of all updates and encryption is September 30, 2016.

AUDITOR-CONTROLLER RECOMMENDATION #7

Ensure damaged and obsolete equipment is properly disposed of and removed from inventory.

Child Support Services Response:

The Child Support Services Department agrees and is in the process of implementing this recommendation. CSSD Chief Technology Office personnel will reanalyze the laptops in question. If they can be repaired and put back into service, they will be brought back online. If they are found to be unrepairable, they will be sent to salvage. Completion of this analysis and possible repair will be completed in September 2016.

AUDITOR-CONTROLLER RECOMMENDATION #8

Evaluate using encryption and antivirus reports along with the IT equipment list, to monitor encryption and antivirus protection on all computing devices.

Child Support Services Response:

The Child Support Services Department agrees and has fully implemented this recommendation. Effective September 2016, the Department Information Security Officer will analyze the current status of encryption and antivirus levels on a monthly basis. Any systems found to not meet the encryption or antivirus standards will be reported to the Technical Support supervisor for remediation.

AUDITOR-CONTROLLER RECOMMENDATION #9

Child Support Services Department management inventory all information technology equipment immediately, and annually thereafter, and update inventory records with the results of the physical counts.

Child Support Services Response:

Child Support Services Department agrees and is in the process of implementing this recommendation. Child Support conducted a department-wide physical barcode scan inventory of all information technology equipment. This scan of all inventory was completed on August 18, 2016. Reconciliation of that inventory will be completed by September 30, 2016. When scanned, the Barcode Inventory Tracking System (AssetWorx!) is updated with the "last observed" date. The Department is committed to conduct an annual physical inventory and maintain updated inventory records.

AUDITOR-CONTROLLER RECOMMENDATION #10

Child Support Services Department management maintain documentation to support the sanitization and donation of computing devices.

Child Support Services Response:

The Child Support Services Department agrees and has fully implemented this recommendation. Regarding the documentation for the sanitization and donation of all computer the following actions have been taken:

- On July 6, 2016, an email containing the CSSD Data Sanitization Policy and the Data Sanitization Form was sent to all Chief Technology Office (CTO) Technical Support personnel. This email outlined the requirements for documentation of these processes. Each member of the team responded to the email with their acknowledgement and understanding of the policy and what was required of them.
- A digital copy of the completed Data Sanitization form for each device will be saved on the CTO file share. A copy of this document will be sent to the Facilities division for their records.
- Once the items have been donated, the Facilities division will send a copy of the proof of donation to the CTO for their records.

AUDITOR-CONTROLLER RECOMMENDATION #11

Child Support Services Department management ensure all employees complete the required Information Security Awareness Training when hired and annually thereafter.

Child Support Services Response:

The Child Support Services Department agrees and is in the process of implementing this recommendation. Regarding the tracking of the completion of the Information Security Awareness Training by all active employees, the following has been confirmed:

- In June 2016, CSSD's Program Support Division received a list of users who had not completed the training from the CSSD Human Resources Division. An email was sent to all supervisors in the department, alerting them as to which of their employees need to take the training. The Program Support Division continue to track the training completion status.
- CSSD will continue to track this issue until all available employees have completed the training.
- Effective January 2017, when the next round of trainings start, the Program Support Division will continue to send notifications to supervisors throughout the department regarding the training completion status for their staff, and the Department Information Security Officer will be assigned responsibility for ensuring that all employees have completed the training.

AUDITOR-CONTROLLER RECOMMENDATION #12

Child Support Services Department management perform risk assessments on all critical systems by properly completing the Internal Control Certification Program.

Child Support Services Response:

The Child Support Services Department agrees with the Auditor-Controller's recommendation and will implement in future ICCPs. CSSD will perform risk assessments on CSE and MEDS by completing the ICCP during the next annual ICCP assessment.